Sale or Transfer of Computers and Software

VERSION 1.0 • 29 NOV 2005

Table of Contents

The current version of 1 Texas Administrative Code Chapter 202, Information Security Standards, is available from the Texas Secretary of State Web site: http://www.sos.state.tx.us.

Executive Summary

This guideline is intended to supplement existing policies and procedures on the sale and transfer of surplus and salvaged equipment. The recommendations contained in this document should be read in the context of the existing laws that regulate this activity.

The sale or transfer of old, obsolete, damaged, nonfunctional, or otherwise unneeded computers, computer peripherals, and computer software presents special problems for state Information Resources Managers (IRMs) and property managers. This guideline identifies several important issues and makes recommendations concerning procedures. This document should not be considered legal advice and all state agencies and institutions of higher education should consult their own attorneys before making changes to any of their existing procedures.

Transfer or Disposition of Data Processing Equipment

The transfer or disposition of data processing equipment, such as computers, is controlled by Texas Government Code § 403.278 (between state agencies), or Texas Government Code Chapter 2175. In general, under Chapter 2175, data processing equipment may be sold to a government entity or assistance organization through the Texas Comptroller of Public Accounts, or, if not sold, may be disposed of to certain organizations provided for in Texas Government Code § 2175.128. Certain governmental entities, such as the Secretary of State; the Legislature; the Texas Department of Criminal Justice; state agencies involved in the areas of health, human services, or education; and institutions of higher education have unique disposition requirements. Legal counsel should always be consulted to determine if the proposed disposition of data processing equipment is in compliance with statutory requirements.

Data and Software on Computer Storage Media

There are at least three major risks involved in allowing hard disks and other computer storage media to be sold or otherwise disposed.

1. VIOLATION OF SOFTWARE LICENSE AGREEMENTS

Most software is licensed for use on either a single computer system, to a single person, or to an organization. Usually these licenses are not transferable. Even when the licenses are transferable, there may be specific requirements that must be met, such as possession of the original distribution media, consent of the licensor, or payment of a transfer fee, in order to effect the transfer. Allowing a third party access to licensed software without proper transfer of the license may be a breach of the license agreement, and may subject the state or the recipient of the software to claims for damages.

2. UNAUTHORIZED RELEASE OF CONFIDENTIAL INFORMATION

State agencies and institutions of higher education are often in the possession of confidential information of various sorts, such as student records protected by the Federal Educational Rights and Privacy Act; medical records protected by, among others, the Americans with Disabilities Act; and personnel information. Allowing an unauthorized person access to confidential information can subject the state, and sometimes individual employees, to claims for damages.

3. UNAUTHORIZED DISCLOSURE OF TRADE SECRETS, COPYRIGHTS, AND OTHER INTELLECTUAL PROPERTY

At state universities and other research organizations within state government, researchers often use computer systems to develop and store data, programs, designs, techniques, etc., that are or will become valuable assets of the state as either trade secrets, copyrighted materials, patented inventions, or other intellectual property. Accidental or premature disclosure could mean a loss of secrecy under trade secrets law or constitute a publication under federal copyright law, either of which might result in loss of the asset.

Disposal of Computers

Often, computers disposed of by state agencies and institutions of higher education are no longer in working condition but may contain hard disk drives or other storage media that might work if moved to a working computer. This means that it is possible that the contents of those media cannot be determined before disposal and might be readable by a third party that receives the computers. In addition, deleting, or even erasing files, from the storage media may not adequately protect the information from a knowledgeable third party who has the capability of restoring deleted or erased files. Data in certain files, including hidden files, caches and logs, may be particularly difficult to locate and erase.

Disposal of Documentation

Often the documentation associated with licensed software is covered by the same license as the software and cannot be transferred to a third party. Software and documentation may not be transferred unless the underlying license permits such transfer, and all requirements in the license for transferring such ownership are strictly adhered to.

Removal of Data from Data Processing Equipment

Under Texas Government Code § 2054.130, state agencies and institutions of higher education are required to permanently remove data from data processing equipment before disposing of or otherwise transferring the equipment to a person who is not a state agency or other agent of the state.

Data can be present on any type of storage device, whether fixed or removable, that contains data and maintains the data after power is removed from the device. Due to the advances in computer forensics, simply deleting the data and formatting the disk will not prevent someone from restoring the data. However, *sanitization* of the storage media removes the information from the media in such a way that data recovery using common techniques or analysis is prevented. The U.S. Department of Defense directive, 5220.22-M, "National Industrial Security Program Operating Manual," states that sanitization of storage media can be accomplished using two different methods:

1. Overwriting *is a software procedure that replaces the data previously stored on magnetic storage media with a predefined set of meaningless data.* At a minimum, overwriting should be done using a character, its complement, then a random character. For restricted personal information, additional overwriting (up to seven passes) using different characters is recommended.

2. Degaussing *(i.e., demagnetizing) is a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more reliable than overwriting magnetic media.*[1]

Free software tools to overwrite data that comply with the 5220.22-M standard for disk-sanitization are available.[2] For additional information on specific tools and procedures to use for different types of storage media see Table 1: Clearing and Sanitization Data Storage, within 5220.22-M, Chapter 8, Section 5, "Software and Data Files".

---

[1] Department of Defense, Chapter 8, Section 5, "National Industrial Security Program Operating Manual" (NISPOM), Washington, D.C. (2004) Retrieved November 22, 2005 at <http://www.dtic.mil/whs/directives/corres/pdf/522022msup1_0295/cp8.pdf>.

[2] These tools are available from The Free Country Web site, <http://www.thefreecountry.com/security/securedelete.shtml>.

Recommendations

To limit the state's liability and risk, unless the agency can absolutely verify that no personal or confidential information, intellectual property, or licensed software is stored on the hard drive/storage media, the hard drive/storage media should be sanitized or be removed and destroyed.

Prior to the sanitization or destruction of the storage media, copies of any official state records should be archived according to state/agency policy (See 13 Texas Administrative Code § 6.95, "Final Disposition of Electronic State Records."[3]

If the agency can verify that no personal or confidential information is stored on the hard drive/storage media and that there is the specific intent and legal right to transfer software or data to the purchaser, copies of the license agreements must accompany the computer equipment, and all requirements in the license for the transferring such ownership must be met. All other programs must be removed or uninstalled.

[3] 13 TEX. ADMIN. CODE § 6.95 (2000) (Texas State Library and Archives Commission) Retrieved November 22, 2005 from the Office of the Texas Secretary of State at <http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=13&pt=1&ch=6&rl=95>.

Texas Department of Information Resources
P.O. Box 13564
Austin, TX 78711-3564
www.dir.state.tx.us